UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/557,628	11/17/2005	Pim Theo Tuyls	NL030552	4463

24737 7590 07/13/2009

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
SIMS, JING F	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
07/13/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/557,628	TUYLS ET AL.	
	Examiner	Art Unit	
	JING SIMS	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 May 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on May 11th has been entered.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite. The preamble of claim 1 claims “a method of generating authentication data”; however, the comprised acts do not include the step or steps of any authentication data being generated. Claim 1 states “inserting the control value V and the criteria W in the authentication data”. Since no authentication data has been generated, this limitation renders the claim indefinite. Examiner examines the limitation as “storing the control value V, the criteria W as authentication data to a storage device”.

4. Claim 14 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite. The preamble of claim 14 claims “a computer program … for generating authentication data…; however, the comprised acts does not define what the authentication includes.

Claim 1 states "insert the control value V and the criteria W in the authentication data"; from this limitation, it says the control value V and the criteria W are part of the authentication data, but the succeeding limitation states "store the control value V, the criteria W and the authentication data to a storage device", therefore, control value V and the criteria W are separate from authentication, which are not part of the authentication data. They are contradicting limitation, and it yields the claims indefinite. Examiner examines the limitation as "output the control value V and the criteria W as the authentication data; and store the control value V, the criteria W as authentication data to a storage device".

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claim 17 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claim 17 claims "an output for supplying the control value V and the criteria W to the storage as part of the authentication data"; however, In Fig. 2A it shows the helper data W and the control value V are stored to an storage as authentication data, therefore, the helper data W and the control value V are authentication data, not only the part of the authentication data. Examiner examines the

corresponding portion in claim 17 as "an output for supplying the control value V and the criteria W to the storage as ~~part of~~ the authentication data".

7. Claims 1, 6, 14, 15, 16, 17 and 18 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claims contain subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The claims include the term "criteria W". In light of the specification, "W" has been described as "helper data W" (page 5, line 7; page 9, line 30, etc); therefore, Examiner examines the term as "the criteria that defined by helper data W".

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. **Claims 15, 16, and 18** are rejected under 35 U.S.C. 102 (b) as being anticipated by Yamaguchi et al (US 6314196) (hereinafter Yamaguchi).

As per **claim 15**, Yamaguchi discloses "a method of authenticating a physical object; the method comprising acts of:

measuring a property set Y of the object using a measurement procedure; creating a property set I from the measured property set Y that meet a predetermined

robustness criterion; creating a property set A from the property set I that includes less information on the actual properties than property set Y; generating a control value V' in dependence on properties of the property set A". The limitations above are identical to a method of generating authentication data in claim 1. To avoid redundancy, all the rejection for claim 1 is also applied to the part of claim 15 above.

Yamaguchi also discloses "retrieving a control value V (col. 19, lines 52-56, checking unit fetches the registered best fingerprint) and criteria W (col. 22, lines 1-6, since the fingerprint checking unit and the fingerprint registering device have a common function in the processing the fingerprint, they can be achieved by the same computer, therefore, the finger checking unit must retrieve same thinning process function as the registering process) that has been generated for the physical object during an enrollment wherein the creating acts are guided by the criteria W; and authenticating the physical object if there is a predetermined correspondence between the generated control value V' and the retrieved control value V" (col. 30, line 25-35, in Fig. 20, flowchart of registering of the register "first fingerprint" in ref. no. A2, and by authenticating the physical object by "match" in ref. no. A5. "The first fingerprinting is effected" means the process of retrieving a control value V. "A predetermined correspondence" are explained as "to judge whether or not they match" in prior art. It discloses "the authentication may in principle be done using the same apparatus as used for the enrollment" in the specification. Fig. 20 in Yamaguchi's application is the example of this model).

As per **claim 16**, Yamaguchi discloses "a computer program stored on a computer readable memory device for authenticating a physical object, the computer program being operative to cause a processor to" (fig. 45, and col. 10, line 7-15, the fingerprint checking device includes a processor, a read-only memory storing a program, a multivalued image memory, a binarized image memory):

measure a property set Y of the object using a measurement procedure; create a property set I from the measured property set Y that meet a predetermined robustness criterion; create a property set A from the property set I that includes less information on the actual properties than property set Y; generating a control value V' in dependence on properties of property set A". The limitations above are identical to a method of generating authentication data in claim 1. To avoid redundancy, all the rejection for claim 1 is also applied to the part of claim 16 above.

Yamaguchi also discloses "retrieving a control value V (col. 19, lines 52-56, checking unit fetches the registered best fingerprint) and criteria W (col. 22, lines 1-6, since the fingerprint checking unit and the fingerprint registering device have a common function in the processing the fingerprint, they can be achieved by the same computer, therefore, the finger checking unit must retrieve same thinning process function as the registering process) that has been generated for the physical object during an enrollment, wherein the creating the property set I and the property set A are guided by the criteria W"; "and authenticating the physical object if there is a predetermined correspondence between a generated control value V' and the retrieved control value V" (col. 30, line 25-35, in Fig. 20, flowchart of registering of the register "first fingerprint" in

ref. no. A2, and by authenticating the physical object by “match” in ref. no. A5. “The first fingerprinting is effected" means the process of retrieving a control value V. "A predetermined correspondence” are explained as “to judge whether or not they match” in prior art. It discloses “the authentication may in principle be done using the same apparatus as used for the enrollment” in the specification. Fig. 20 in Yamaguchi’s application is the example of this model).

As per **claim 18**, Yamaguchi discloses “an authentication device for authenticating a physical object, the authentication device comprising” (col. 17, line 3-4, Yamaguchi discloses “the embodiment of a fingerprint checking device”):

“an input for receiving a property set Y of a physical object measured using a measurement procedure” (Fig. 1, ref. no. 1, fingerprint image pickup unit), “and for receiving a control value V (fig. 2, reference A11, the control value V appears to be best finger selection; reference A7 shows the best finger selection has been stored) and a criteria W from a storage” (col. 22, lines 1-6, since the fingerprint checking unit and the fingerprint registering device have a common function in the processing the fingerprint, they can be achieved by the same computer, therefore, the finger checking unit must retrieve same thinning process function as the registering process);

“a processor for creating a property set I from the measured property set Y that meet a predetermined robustness criterion” (col. 18, lines 58, wherein the digitized/binarized fingerprint image corresponding with property set I; col. 4, lines 27-33, describe the criteria to digitize the image; it also shows in fig. 1, ref. 10, property set I appears to be the data that after binarized image converting unit process), “for creating

a property set A from the property set I that includes less information on the actual properties than property set Y" (col. 18, lines 61-63, wherein the binarized fingerprint image after thinning-processed corresponding to property set A; col. 2, lines 8-14, the thinning process, also in fig. 32 B, the binarized fingerprint image after thinning process shows less distracting information than the original fingerprint image in fig. 32A), "wherein the creating the property set I and the property set A are guided by a criteria W" (col. 18, lines 61-63, wherein the thinning process corresponding with criteria W, or col. 4, lines 27-33, and line 52-61, Fig. 36, the creating acts are guided by a criteria W as m and/or n. M and n control the selection of the subsets which are the divided image blocks. Thereby limit the range of parameters (finger print pattern) which is the criteria that guides the creating acts); "for generating a control value V' in dependence on properties of the property set A" (fig. 2, ref. no. A11, control value V appears to be the best finger selection. The best fingerprint selection is based on result after thinning); "and for authenticating the physical object if there is a predetermined correspondence between the generated a control value V' and the retrieved control value V and an output for issuing a signal indicating whether or not the physical object has been authenticated" (Fig. 1, reference 5, "checking unit" and/or "judging unit"; fig. 20, ref. no. A5, the issued signal appears to be the signal after the process of match).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1-6, 14, and 17 are rejected under 35 U.S.C 103(a) as being unpatentable over Yamaguchi, in view of Kobayashi (US Patent 7093131 B1).

As per **claims 1 and 14**, Yamaguchi discloses "a method of generating authentication data for authenticating a physical object; the method comprising acts of" *(col. 1, line 7-8, a fingerprint registering method for registering a fingerprint; col. 1, line 32-33, to authenticate personal identification)*; and "a computer program stored on a computer readable memory device for generating authentication data for authenticating a physical object, the computer program being operative to cause a processor to" (fig. 45, and col. 10, line 7-15, the fingerprint checking device includes a processor, a read-only memory storing a program, a multivalued image memory, a binarized image memory):

"measuring a property set Y of the object using a measurement procedure" (col. 18, lines 53-57, wherein fingerprint image of a fingerprint corresponding with property set Y of the object; also fig. 1, ref. no. 1, Yamaguchi discloses this limitation as "fingerprint image pickup unit" a fingerprint image is property set, and the pickup unit certainly performing a measurement procedure to pickup the fingerprint);

"creating a property set I from the measured property set Y that meet a predetermined robustness criterion" (col. 18, lines 58, wherein the digitized/binarized fingerprint image corresponding with property set I; col. 4, lines 27-33, describe the

criteria to digitize the image; it also shows in fig. 1, ref. 10, property set I appears to be the data that after binarized image converting unit process);

"creating a property set A from the property set I that includes less information on the actual properties than property set Y" (col. 18, lines 61-63, wherein the binarized fingerprint image after thinning-processed corresponding to property set A; col. 2, lines 8-14, the thinning process, also in fig. 32 B, the binarized fingerprint image after thinning process shows less distracting information than the original fingerprint image in fig. 32A), "wherein the creating acts are guided by a criteria W" (col. 18, lines 61-63, wherein the thinning process corresponding with criteria W, or col. 4, lines 27-33, and line 52-61, Fig. 36, the creating acts are guided by a criteria W as m and/or n. M and n control the selection of the subsets which are the divided image blocks. Thereby limit the range of parameters (finger print pattern) which is the criteria that guides the creating acts);

"generating a control value V in dependence on properties of property set A (fig. 2, ref. no. A11, control value V appears to be the best finger selection. The best fingerprint selection is based on result after thinning);

"inserting the control value V in the authentication data" (col. 1, lines 17-19, wherein the registered fingerprint corresponding with control value V, and the fingerprint is the authenticate data to authenticate personal ID), "and storing the control value V to a storage device" (col. 29, lines 7-13, the registered fingerprint data is stored in the file).

However, Yamaguchi does not explicitly disclose "inserting the criteria W in the authentication data; and storing the criteria W to a storage device".

Kobayashi discloses “inserting the criteria W in the authentication data” (col. 16, line 42-49, and Fig. 3, S116, wherein the time, positional, environmental condition, personal, and apparatus information corresponding with the criteria W); “and storing the criteria W to a storage device” (fig. 3, step S128, store digital data in data store unit).

Yamaguchi and Kobayashi are analogous art because they are from the same field of endeavor of a method and apparatus for processing and authenticating input digital information.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the criteria W which is the thinning process for the fingerprint image as described by Yamaguchi and add the time information, the extra positional information, e.g. horizontal or vertical of the image, environmental condition information, personal information and the apparatus information, e.g. the serial number of the fingerprint image pickup apparatus as taught by Kobayashi during/after the thinning process, because it would add the complexity of the authentication which is the fingerprint image, therefore improve the security of the authentication system.

As per **claim 2**, Yamaguchi discloses "the method as claimed in claim 1, wherein the act of creating the property set A includes performing a contracting transformation that transforms given ranges of input properties to corresponding output values” (Fig. 3, ref. no. B4, Yamaguchi discloses as “extract minutiae”. The process of “extracting minutiae” is to transform a biometric data - for example a fingerprint - from one state to the other state by performing “extract minutiae”. The input properties range is the

thinning processed image and the output values are the minutiae are the detected minutia based on the thinning processed image in col. 20, line 61-63,).

As per **claim 3**, Yamaguchi discloses "the method as claimed in claim 1, wherein the contracting transformation transforms a property to a binary number representative of whether the property has a positive or negative value" (Fig. 17, ref. no. A8, and col. 29, line 7-8 "the content d at the n-th byte of the registered fingerprint data is stored in the register (A8)" Yamaguchi discloses the content in "byte", it is the length unit used by binary numbers, therefore, "a property" is represented by binary numbers. Transforming a property to binary number representative of whether the property has a positive or negative value is well known technology in the art, for example, US Patent 3,947,876 discloses "to convert the positive and negative data transitions to binary ones and zeros respectively" (see Gary, col. 7, line 50-54)).

As per **claim 4**, Yamaguchi discloses "the method as claimed in claim 1, wherein the act of creating the property set A includes an act of selecting a subset of the property set I" (col. 4, line 27-30 and line 52-61, Yamaguchi discloses an self-explanatory diagram in Fig. 36, Yamaguchi also explains "dividing a pictured image into blocks, and when 512.times.512 picture elements are determined as one screen, division into 1024 blocks is made with 16.times.16 picture elements as one block"; therefore, the blocks have the equal meaning with "subsets" in the instant application. Yamaguchi further discloses "selecting a subset" as in Fig. 38, and give the example of "the flowchart of a conventional example". It is an actually selecting process of subsets in Yamaguchi's application).

As per **claim 5**, Yamaguchi discloses "the method as claimed in claim 4, including an act of creating criteria W for controlling the selection" (col. 4, line 27-33, and line 52-61, Fig. 36 are an self-explanatory diagram of dividing a pictured image into blocks, the subset has been described as blocks "in which a block number is initialized with m=1 (B-1). In other words, number m for 1 to 1024 is allocated with respect to 1024 blocks in the image shown in FIG. 36, and the block number m is determined as 1 for initialization. Then, with n=1 (B2), the picture element number n in the block is initialized. In other words, the number n for 256 picture elements in the image shown in FIG. 36 is allocated, and this picture element number n is determined as 1 for initialization." Yamaguchi discloses the "criteria W" in the application appears to be m or/and n. M and n controls the selection of the subsets which are the divided image blocks. Thereby limit the range of parameters (finger print pattern) which is the criteria that controls the selection).

As per **claim 6**, Yamaguchi discloses "the method as claimed in claim 5, including an act of creating unique criteria W based on respective authentication applications" (col. 3, line 57-67, Yamaguchi discloses "based on the multivalued image, it is judged by the fingerprinting judging unit 313" "division into respective blocks is made". Yamaguchi discloses earlier "block number m and picture element number n", so m is block number. It indicates from above statements that the block number m is based on the multivalued image. The multivalued image is generated upon the fingerprint by the fingerprint image pickup unit 311. Therefore, the block number m is uniquely created respect to each authentication applications), "wherein different

respective authentication applications have different unique criteria" (m and n are variables. The example in col. 4, line 52-61, m has been set to 1-1024, and n has been set to 1-256; however, Yamaguchi also discloses the criteria can be changed due to different applications in col. 4, line 5-8, as the process of determining the luminance of the focused picture element can be made with respect to blocks. In col. 3, line 64-67, it indicates the block can be 16x16 or others, which indicates the criteria/variables m and n may be changed based on the luminance of each application).

As per **claim 17**, Yamaguchi discloses "a system for authenticating a physical object" (col. 17, line 3-4, Yamaguchi discloses "the embodiment of a fingerprint checking device") "the system including an enrollment device" (Fig. 1, ref. no. 1 Yamaguchi discloses as "image pickup unit"); "an authentication device" (Fig. 1, ref. no. 1, Yamaguchi discloses as "image pickup unit". The specification of the instant application discloses that the authentication may in principle be done using the same apparatus as used for the enrollment, therefore, authentication device also can be "image pickup unit") "and a storage for storing authentication data" (Fig. 1, reference unit 6, Yamaguchi discloses as "registering unit", it also can be find in Fig. 20, ref. no. A3, Yamaguchi discloses as "temporary fingerprint registering");

"the enrollment device including: an input for receiving a property set Y of the object measured using a measurement procedure" (fig. 1, ref. no. 1, fingerprint image pickup unit);

"a processor for creating a property set I from the measured property set Y that meet a predetermined robustness criterion" (col. 18, lines 58, wherein the

digitized/binarized fingerprint image corresponding with property set I; col. 4, lines 27-33, describe the criteria to digitize the image; it also shows in fig. 1, ref. 10, property set I appears to be the data that after binarized image converting unit process), "creating a property set A from the property set I that includes less information on the actual properties than property set Y" (col. 18, lines 61-63, wherein the binarized fingerprint image after thinning-processed corresponding to property set A; col. 2, lines 8-14, the thinning process, also in fig. 32 B, the binarized fingerprint image after thinning process shows less distracting information than the original fingerprint image in fig. 32A), "wherein the creating the property set I and the property set A are guided by a criteria W" (col. 18, lines 61-63, wherein the thinning process corresponding with criteria W, or col. 4, lines 27-33, and line 52-61, Fig. 36, the creating acts are guided by a criteria W as m and/or n. M and n control the selection of the subsets which are the divided image blocks. Thereby limit the range of parameters (finger print pattern) which is the criteria that guides the creating acts); "and generating a control value V in dependence on properties of the property set A and the criteria W" (fig. 2, ref. no. A11, control value V appears to be the best finger selection. The best fingerprint selection is based on result after thinning. Best fingerprint also depends on the thinning process);

"and an output for supplying the control value V to the storage as part of the authentication data" (29, lines 7-13, the registered fingerprint data is stored in the file);

"and the authentication device including: an input for receiving a property set Y' of the object measured using a measurement procedure and for receiving the control value V from the storage including the criteria W; a processor for creating a property set

I' from the measured property set Y' that meet a predetermined robustness criterion; for creating a property set A' from the property set I' that includes less information on the actual properties than property set Y', wherein the creating the property set I' and the property set A' are guided by the criteria W; for generating a control value V' in dependence on properties of the property set A'" (since the specification of the instant application discloses that the authentication may in principle be done using the same apparatus as used for the enrollment, therefore, see the rejection to claims 1 or 15, for the corresponding sections); "for authenticating the physical object if there is a predetermined correspondence between the generated a control value V' and the retrieved control value V and an output for issuing a signal indicating whether or not the physical object has been authenticated" (Fig. 1, reference 5, "checking unit" and/or "judging unit"; fig. 20, ref. no. A5, the issued signal appears to be the signal after the process of match).

However, Yamaguchi does not explicitly disclose "output the criteria W to a storage device and part of the authentication data".

Kobayashi discloses "inserting the criteria W in the authentication data" (col. 16, line 42-49, and Fig. 3, S116, wherein the time, positional, environmental condition, personal, and apparatus information corresponding with the criteria W); "and storing the criteria W to a storage device" (fig. 3, step S128, store digital data in data store unit).

Yamaguchi and Kobayashi are analogous art because they are from the same field of endeavor of a method and apparatus for processing and authenticating input digital information.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the criteria W which is the thinning process for the fingerprint image as described by Yamaguchi and add the time information, the extra positional information, e.g. horizontal or vertical of the image, environmental condition information, personal information and the apparatus information, e.g. the serial number of the fingerprint image pickup apparatus as taught by Kobayashi during/after the thinning process, because it would add the complexity of the authentication which is the fingerprint image, therefore improve the security of the authentication system.

12. Claims 7, 9, 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over anticipated by Yamaguchi (US 2001/6314196), in view of Ort et al. (US 5799098) (hereinafter Ort).

As per **claim 7**, Yamaguchi discloses “the method as described in claim 1”, but fails to disclose "wherein the predetermined robustness criterion is based on a signal to noise ratio of the measured properties and the act of creating the property set I includes performing a transformation .GAMMA. on the property set Y to create two disjunct property sets I.sub.1 and I.sub.2 where a signal to noise ratio of properties of the property set I.sub.1 are estimated to be higher than a signal to noise ratio of properties of I.sub.2; and using I.sub.1 as the property set I.”

However, Ort discloses the limitations (col. 14, line 29-41, Ort uses “filter 110” and “filter 120” to serve the functionalities of transformation Γ. “The two disjunct property set I.sub.1 and I.sub.2” are described as the output data I.sub.FSCE after the

process of contrast enhancement in fig. 7, ref. no. 120 and the output data I.sub. FS after the process of low pass filter (Fig. 7 ref. no. 110 respectively. It is obvious for one skilled in the art to observe that I.sub.FSCE has higher Signal to noise ratio than the output data I.sub. FS after the process of low pass filter in Fig. 7 reference 110 and the purpose of this transformation is to produce a higher signal to noise ratio.)

Yamaguchi and Ort are analogous art because they are from the same field of using biometric data, which in both applications are fingerprints to enhance the image of fingerprint quality by eliminating the noise, and get a higher signal to noise ratio.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teaching of Yamaguchi to use the low filter and contrast enhancement of Ort because it would provide to enforce the robust criterion, then to further consolidate the security of the system by applying the techniques to lessen the contained information in Yamaguchi.

As per **claim 9**, Ort discloses "the method as claimed in claim 7, including the act of creating the transformation .GAMMA. in dependence on a statistical property of the measurement procedure" (col. 14, line 28-41, Ort discloses the statistical property in the term of "high frequency noise". The high frequency noise data is obviously generated during the measurement procedure.)

As per **claim 10**, Ort discloses "the method as claimed in claim 9, wherein the statistical property includes a covariance matrix derived from estimated properties X of the object and a corresponding statistical distribution F determined during the measuring the property set Y" (col. 14, line 20-41, Ort discloses estimated properties X

to be “ridge angle”, and corresponding statistical distribution F appears to be "an 800 by 800 pixel image". It is obvious for one skilled in the art that both of the data sets are represented by matrices. The 800 by 800 pixel image is determined during the measuring of the original physical object).

As per **claim 11**, Ort discloses “the method as claimed in claim 7, including an act of deriving a threshold from a noise level in the measured property set and assigning created properties with an absolute value larger than the threshold to set I.sub.1” (col. 29, line 43-50, with respect to this limitation, Ort discloses “The 256 cells of Q.sub.coarse are filled by sequentially considering the data within each of 256 16.times.16 cell submatrices of Q.sub.smooth that in total comprise all the cells of it. Each of the 16 cells within a submatrix are examined to determine if the stored cell value is below a fixed poor quality threshold. If 75% of the cells are below a quality of 0.5 for Q.sub.coarse, then the cell is dubbed as poor quality. If 75% (12 cells) are below the threshold then: the corresponding Q.sub.coarse (i,aj) is set to 0; otherwise Q.sub.coarse (i,j) is set to 1.” Ort discloses the same concept of deriving a threshold from the percentage of measured property set by using the term “Q.sub.coarse”).

13. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yamaguchi, in view of Ort, and further in view of Vizcaya (Pedro Vizcaya, A personnel identity verification method using DAB fingerprints (Pattern recognition), 1998).

As per **claim 8**, Yamaguchi and Ort disclose a method as claimed in claim 7 but do not specifically teach wherein the transformation .GAMMA. is a linear transformation that converts a vector representing the property set Y to a vector with components as representing the set I, where each vector component .alpha..sub.i is independent of the other vector components .alpha..sub.j (j.noteq.i) and wherein the vector components are sorted according to an estimated signal to noise ratio.

However, Vizcaya discloses “a linear transformation” (Page ix, line 19-23, “a linear transformation” by “since model is linear, its parameters are efficiently calculated using standard linear transform techniques. Additionally, the model allows the evaluation of the specific contribution of each singularity to explain the ridge orientation everywhere”) “that converts a vector representing the property set Y to a vector with components as representing the set I, where each vector component .alpha..sub.i is independent of the other vector components .alpha..sub.j (j.noteq.i) and wherein the vector components are sorted according to an estimated signal to noise ratio” Using independent vectors with sorted order to represent a physical object (i.e. property set) is well known and expected in the art.

Yamaguchi, Ort, and Vizcaya are all analogous art because they are all from the same field of enhancing the biometric data, which in these three cases specifically fingerprints, by extracting the key feature to get a higher signal to noise ratio, to authenticate an access.

It would have been obvious to one of ordinary skill in the art at the invention time to modify the teaching of Yamaguchi in view of Ort for applying the linear transformation

algorithm of Vizcaya because it would provide for the transformation of a vector to the other vectors in more rapid fashion, therefore, to shorten the authentication processing time.

14. Claims 12 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamaguchi in view of Bjorn (US 6035398).

As per **claim 12**, Yamaguchi discloses "the method as claimed in claim 1, wherein the act of creating the control value V" [see rejection to claim 1 above], and "converting each property of the property set A into a binary digit" (transforming a property to binary number representative of whether the property has a positive or negative value is well known technology in the art, for example, US Patent 3,947,876 discloses "to convert the positive and negative data transitions to binary ones and zeros respectively" (see Gary, col. 7, line 50-54)), but fails to disclose "includes acts of performing a cryptographic function on properties of the property set A".

However, Bjorn discloses "performing a cryptographic function on a combination of the binary digits" (col. 4, line 25-37, and Fig. 3, ref. no. 325, Hash template to create cryptographic key, at block 325, "the template is hashed. For one embodiment, this hash is the cryptographic key. For another embodiment, known techniques are used on the hash to generate the cryptographic key. This cryptographic key is identified with the specific fingerprint, and thus with a specific user". It is known that cryptographic function is performed on combination of the binary code at the invention time).

Yamaguchi and Bjorn are analogous art because they are from the same field of using biometric data to enhance authentication process.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teaching of Yamaguchi to apply the one-way hash function of Bjorn because it would provide to generate a cryptographic key to enhance the security of control value V in Yamaguchi for the authentication.

As per **claim 13**, Bjorn discloses claim 13 “the cryptographic function is a one-way function” (col. 4, line 25-37, and Fig. 3 ref. no. 325 Hash template to create cryptographic key, at block 325, the template is hashed. For one embodiment, this hash is the cryptographic key. For another embodiment, known techniques are used on the hash to generate the cryptographic key. This cryptographic key is identified with the specific fingerprint, and thus with a specific user”).

Response to Arguments

15. Regarding to Applicants’ Remarks that corresponding with claim 1 on page 10, Applicants argued that Yamaguchi fails discloses or suggest "inserting the control value V and the criteria W in the authentication data". In the new round of the rejection, the control value V is corresponding with the registered fingerprint in Yamaguchi’s application, therefore, the registered fingerprint is a part of the authentication data. The criteria W is corresponding with the thinning process in Yamaguchi. Yamaguchi does not explicitly discloses insert the process of thinning fingerprints into the authentication data; however, Kobayashi discloses add time, positional, environmental condition,

personal, and apparatus information to digital data as authentication information (col. 16, line 42-49, and Fig. 3, S116). Yamaguchi and Kobayashi are analogous art. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the criteria W which is the thinning process for the fingerprint image as described by Yamaguchi and add the time information, the extra positional information, e.g. horizontal or vertical of the image, environmental condition information, personal information and the apparatus information, e.g. the serial number of the fingerprint image pickup apparatus as taught by Kobayashi during/after the thinning process, because it would add the complexity of the authentication which is the fingerprint image, therefore improve the security of the authentication system.

16. Regarding to Applicants' Remarks that corresponding with claim 1 on page 10, Applicants also argued that neither the storing of the inspection information nor the storing of the authenticating information discloses or suggests "inserting the control value V and the criteria W in the authentication data". However, in the new round of the rejection, Yamaguchi discloses "inserting the control value V in the authentication data" (col. 1, lines 17-19, wherein the registered fingerprint corresponding with control value V, and the fingerprint is the authenticate data to authenticate personal ID), "and storing the control value V to a storage device" (col. 29, lines 7-13, the registered fingerprint data is stored in the file); Kobayashi discloses "inserting the criteria W in the authentication data" (col. 16, line 42-49, and Fig. 3, S116, wherein the time, positional, environmental condition, personal, and apparatus information corresponding with the criteria W); "and storing the criteria W to a storage device" (fig. 3, step S128, store

digital data in data store unit); therefore, Yamaguchi in view of Kobayashi disclose the limitations.

17. On page 11 of the Applicants' Remarks also corresponding with claim 1, Applicants argued that the authenticating information from Kobayachi is just additional information added to the digital picture data and does not disclose or suggest the inserting the criteria W and the control value V in the authentication data; however, Yamaguchi discloses "insert control value V" as authentication data, and Kobayachi teaches the time, positional, environmental condition, personal, and apparatus information is not only the additional information, but also criteria to guide the authentication process (fig. 5, S204, S206, S212, S218) and for one ordinary skilled in the art then environmental condition, and the apparatus information can help with process of thinning process of Yamaguchi which is the process to create the authentication data in the instant application.

18. To responds to the remarks on page 11 last paragraph that also corresponding with claim 1, Yamaguchi discloses "creating a property set I from the measured property set Y that meet a predetermined robustness criterion" (col. 18, lines 58, wherein the digitized/binarized fingerprint image corresponding with property set I; col. 4, lines 27-33, describe the criteria to digitize the image; it also shows in fig. 1, ref. 10, property set I appears to be the data that after binarized image converting unit process); "creating a property set A from the property set I that includes less information on the actual properties than property set Y" (col. 18, lines 61-63, wherein the binarized fingerprint image after thinning-processed corresponding to property set A; col. 2, lines 8-14, the

thinning process, also in fig. 32 B, the binarized fingerprint image after thinning process shows less distracting information than the original fingerprint image in fig. 32A), "wherein the creating acts are guided by a criteria W" (col. 18, lines 61-63, wherein the thinning process corresponding with criteria W, or col. 4, lines 27-33, and line 52-61, Fig. 36, the creating acts are guided by a criteria W as m and/or n. M and n control the selection of the subsets which are the divided image blocks. Thereby limit the range of parameters (finger print pattern) which is the criteria that guides the creating acts);

"generating a control value V in dependence on properties of property set A (fig. 2, ref. no. A11, control value V appears to be the best finger selection. The best fingerprint selection is based on result after thinning);

"inserting the control value V in the authentication data" (col. 1, lines 17-19, wherein the registered fingerprint corresponding with control value V, and the fingerprint is the authenticate data to authenticate personal ID), "and storing the control value V to a storage device" (col. 29, lines 7-13, the registered fingerprint data is stored in the file).

However, Yamaguchi does not explicitly disclose "inserting the criteria W in the authentication data; and storing the criteria W to a storage device".

Kobayashi discloses "inserting the criteria W in the authentication data" (col. 16, line 42-49, and Fig. 3, S116, wherein the time, positional, environmental condition, personal, and apparatus information corresponding with the criteria W); "and storing the criteria W to a storage device" (fig. 3, step S128, store digital data in data store unit).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JING SIMS whose telephone number is (571)270-7315. The examiner can normally be reached on 7:30am-5:00pm EST, Mon-Thu.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JING SIMS/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437